

EXHIBIT H

From: Brown, Timothy [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=A1BCD95116E84D6692DD89F9D55C5B7A-BROWN, TIMO]
Sent: 12/28/2020 8:21:44 PM
To: McClendon, Lee [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=85d7621555424a70a57a695496a1ee54-McClendon,]; LeCompte, Denny [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4b548c7124334a84a08c7f10f1686ddd-denny lecom]
Subject: RE: Approved response to the "solarwinds123" incident with the update server

With that credential they could upload anything to downloads.solarwinds.com. I have assumed this was our main download site. In their POC they uploaded a file to the site. I have made an assumption that this is our main download site since Lee Zimmerman needed to confirm the download site with on internal checksums.

The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.

This was managed and resolved quickly but it did take place and a very weak password existed to access that environment.

From: McClendon, Lee <Lee.McClendon@solarwinds.com>
Sent: Monday, December 28, 2020 2:08 PM
To: LeCompte, Denny <denny.lecompte@solarwinds.com>; Brown, Timothy <timothy.brown@solarwinds.com>
Subject: Re: Approved response to the "solarwinds123" incident with the update server

Where exactly could someone upload content on Akamai? Did they have the ability to replace legitimate SolarWinds files or was this just a means to send files to us? Were they able to view other files on the download site with these credentials?

This statement in the incident is the one that I don't understand: "I was able to upload a test POC. Via this any hacker could upload malicious exe and update it with release SolarWinds product."

Is this saying that someone could do the following:

- Upload an executable file with a SolarWinds-like name to downloads.solarwinds.com
- Get someone to click on a link to the file by emailing it to them (the user thinks they are running a legitimate SolarWinds file because it was on our download site)
- User installs bad stuff (even though it isn't signed by SolarWinds)

Lee

From: LeCompte, Denny <denny.lecompte@solarwinds.com>
Date: Monday, December 28, 2020 at 1:49 PM
To: Brown, Timothy <timothy.brown@solarwinds.com>
Cc: McClendon, Lee <Lee.McClendon@solarwinds.com>
Subject: RE: Approved response to the "solarwinds123" incident with the update server

Tim – can you provide some more information? We continue to get this one. I'd like to write I up, but I don't understand enough.

I can jump on a call if that would be faster for you.

From: LeCompte, Denny

Sent: Wednesday, December 23, 2020 7:14 PM

To: Brown, Timothy <timothy.brown@solarwinds.com>; Bliss, Jason <Jason.Bliss@solarwinds.com>; Thompson, Kevin <Kevin.Thompson@solarwinds.com>

Subject: RE: Approved response to the "solarwinds123" incident with the update server

Redacted

From: Brown, Timothy <timothy.brown@solarwinds.com>

Sent: Wednesday, December 23, 2020 6:55 PM

To: Bliss, Jason <Jason.Bliss@solarwinds.com>; LeCompte, Denny <denny.lecompte@solarwinds.com>; Thompson, Kevin <Kevin.Thompson@solarwinds.com>

Subject: RE: Approved response to the "solarwinds123" incident with the update server

Redacted

<https://cp.solarwinds.com/display/OP/2019-462%3A+GitHub+Public+Repo+FTP+Credentials+Leakage>

Summary:

On 19 Nov 2019 PSIRT received a report from an external researcher about hardcoded credentials in one of publicly available GitHub repos.

Hi Team,

I have found a public Github repo which is leaking ftp credential belongs to SolarWinds.

Repo URL:

<https://github.com/xkozus00/mib-importer/blob/master/Src/Lib/PurgeApp/PurgeApp.exe.config>

Downloads Url:

<http://downloads.solarwinds.com> FTP Url: <ftp://solarwinds.upload.akamai.com> Username: solarwindsnet
Password: solarwinds123

POC:

<http://downloads.solarwinds.com/test.txt>

I was able to upload a test POC. Via this any hacker could upload malicious exe and update it with release SolarWinds product.

Root Cause Analysis (RCA)

What Happened?	Engineering intern was working on MIB upload functionality improvements. He used the code as a project for his bachelor thesis. He accidentally uploaded it to Github including configuration file that contained login and password for publishing files to Akamai.
Why it Happened	There was no bad intention, it happened accidentally and was also related to juniority of the intern who did not think about it properly before the publishing.
What controls were put in place?	There will be special training introduce to ensure something like that does not happen anymore.
Describe any Lessons Learned	Junior team members and especially interns who are with us only for a while need to be well trained and supervised to ensure, not security breach happens anymore.

Incident Tracking Log

No.	Date/Time	Action	Status	Owner	Notes
1	19 Nov 2019	Report	Complete	Sejna, Tomas	Report received

					from an external researcher.
2	19 Nov 2019	Validation	Complete	Sejna, Tomas	Validate by Pohorelsky, Pavel , IR kick off.
3	19 Nov 2019	Eradication	Complete	Zila, Josef	The compromised account was disabled on Akamai. It was already a backup account, not the main one, so no immediate problem was attached to disabling it. Also, based on logs from Akamai, during the process of disabling it (it took about 6 hours because of their maintenance and distribution on all nodes), no one accessed Akamai using this account other than members of internal release management team
4	21 Nov 2019	Eradication	Complete	Pohorelsky, Pavel	Mentioned project that contained the file was deleted from Github completely and is not available anymore.
5	21 Nov 2019	Recovery	Complete	Zimmerman, Lee	Release management is in the process of verification, if any files present on the Akamai haven't been changed. Because all of the

					are signed by our certificate, the probability is very low. However, just to be 100% sure, release management team is comparing the checksums of files on the internal share with those on Akamai to ensure there no modified files. This will take time, because there is about 2,5 TB of files. As of February 3rd release management has eliminated all but 40 files for us to manually check. This should complete by mid Feb. all indication at this point is that we had no tampering of files.
6	24 Feb 2020	Closure	Complete	Sejna, Tomas	All checksums finished without any discrepancy, closing.

From: Bliss, Jason <Jason.Bliss@solarwinds.com>
Sent: Wednesday, December 23, 2020 5:37 PM
To: LeCompte, Denny <denny.lecompte@solarwinds.com>; Thompson, Kevin <Kevin.Thompson@solarwinds.com>
Cc: Brown, Timothy <timothy.brown@solarwinds.com>
Subject: RE: Approved response to the "solarwinds123" incident with the update server

Redacted

From: LeCompte, Denny <denny.lecompte@solarwinds.com>
Sent: Wednesday, December 23, 2020 11:37 AM

To: Thompson, Kevin <Kevin.Thompson@solarwinds.com>; Bliss, Jason <Jason.Bliss@solarwinds.com>

Subject: FW: Approved response to the "solarwinds123" incident with the update server

Redacted

From: Reves, Joe <joe.reves@solarwinds.com>

Sent: Wednesday, December 23, 2020 11:26 AM

To: Business Escalation <BusinessEscalation@solarwinds.com>

Cc: LeCompte, Denny <denny.lecompte@solarwinds.com>; Shopp, Brandon <brandon.shopp@solarwinds.com>

Subject: Approved response to the "solarwinds123" incident with the update server

Renewals Is getting hit hard for a response to queries about the incident reported by Vinoth Kumar, with an insecure password on our update server. The media is running with this, and it's getting quite a bit of traction. We need an approved response.

See https://www.theregister.com/2020/12/16/solarwinds_github_password/, <https://www.newsweek.com/solarwinds-update-server-could-accessed-2019-using-password-solarwinds123-report-1554986>, <https://www.techdirt.com/articles/20201215/13203045893/security-researcher-reveals-solarwinds-update-server-was-secured-with-password-solarwinds123.shtml>, <https://www.extremetech.com/computing/318430-security-researcher-solarwinds123-password-left-firm-vulnerable-in-2019>, etc.

This is a good candidate for the FAQ. It's coming up that frequently.

joer

Joe Reves

Product Manager, Principal

joe.reves@solarwinds.com

Office: +1 512.682.9321 | Mobile: +1 719.201.6639